UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)))	
v.	))	24-CR-10011 (IT)
CHUKWUNONSO OBIORA, a/k/a "Nonso Obiora,"	))))	
Defendant	))	

<u>SENTENCING MEMORANDUM OF THE UNITED STATES</u>

"Our company had been struggling during the pandemic ... and this loss worsened the situation. The sum [stolen] is equivalent to one month salary of all [of our] employees."

- *Victim 7401798*

"The impact of this crime has been devastating to [our business]. It has shaken the very foundation of trust that we have carefully built with our suppliers over decades. Internally, it has forced us to re-evaluate and overhaul our procedures, leading to a significant increase in the time and resources required to verify and process transactions. ... As an employee-owned company, the financial loss has been a particularly hard blow for us."

- *Victim 7401787*

Over the past decade, business email compromise ("BEC") frauds have become a $55 billion problem.[1] BEC crimes involve hackers who use sophisticated online techniques to trick legitimate businesses into wiring (and losing) their money. But these frauds only work because of defendants like Chukwunonso Obiora, who created and oversaw a network that spirited BEC proceeds through and out of the United States banking system before the victim companies realized that they had been duped. Obiora was a prolific launderer—one who could command

---

[1] Federal Bureau of Investigation, Public Service Announcement, "Business Email Compromise: The $55 Billion Scam", (Sept. 11, 2024) https://www.ic3.gov/PSA/2024/PSA240911 (visited Dec. 11, 2024).

(and share with his network of co-conspirators) overall fees of between 40 and 60 percent of the amounts that hackers stole. In just over two and one-half years, Obiora directed some $6.5 million into bank accounts that he and his co-conspirators controlled. Dozens of victims lost more than $3.3 million.

On June 14, 2024, Obiora pled guilty to a two-count Superseding Information that charged him with conspiracy to obtain a United States passport through false statements, in violation of 18 U.S.C. § 371 (Count 1), and money laundering conspiracy, in violation of 18 U.S.C. § 1956 (Count 2). The Court has scheduled sentencing for December 18, 2024 at 2:30 p.m. The Probation Office's Presentence Investigation Report ("PSR") assigns Obiora a total offense level of 31 and to Criminal History Category VI, with a resulting advisory Guidelines Sentencing Range of 188 to 235 months (or between approximately 15 and 20 years in prison). (¶¶ 133, 176).[2] Pursuant to the government's plea agreement with Obiora, and for the reasons set forth below, including the scale of Obiora's offense, his substantial criminal history, the need to deter this kind of crime generally, and the fact that Obiora orchestrated most of the conspiracy after being removed from the United States to Nigeria, the United States respectfully requests that the Court sentence Obiora to 168 months in prison, which is approximately 10 percent below the bottom of the advisory Guidelines Sentencing Range. The Court should also order 36 months of supervised release, forfeiture, a mandatory special assessment of $200, and that Obiora pay restitution of $3,326,014.48 to the victims in this case. The government does not seek a fine, as Obiora does not appear to have the ability to pay one.

---

[2] All references to the PSR are denoted by the ¶ symbol.

A.   *The Offenses -- The Money Laundering Conspiracy*

BEC schemes are a type of fraud targeting victim companies that make and receive

payments by wire transfer. In a typical BEC scheme, cybercriminals obtain unauthorized access

to a victim company's computer or email network, and they use that access to familiarize

themselves with the victim company's accounts payable or receivable, recurring payments, or

scheduled financial transactions. Cybercriminals then send fraudulent emails to the victim

company that appear to come from a trusted source, such as a creditor, a counterparty to a

transaction, or an accounting supervisor. The fraudulent emails request changes to wiring and

other payment instructions that result in victim companies sending money to bank accounts

controlled by participants in the BEC scheme. (¶ 12). In Obiora's case, cybercriminals targeted

businesses throughout the United States and around the world for BEC scams. (¶¶ 13-17).

Obiora was born in Nigeria, but he moved to the United States at age three. (¶ 142).

Between at least as early as September 2020 and May 2023, Obiora recruited friends and

acquaintances in the Boston area and elsewhere to receive and withdraw proceeds of BEC scams

from bank accounts that the conspiracy controlled, to deposit some of those proceeds into other

bank accounts, to convert some of the proceeds to cash, and to wire some of the proceeds

overseas, all as part of an effort to conceal that the funds were the proceeds of criminal activity.

(¶ 27).

The object of the conspiracy was for Obiora and his co-conspirators to earn a percentage

of the money that victims unwittingly wired at the hackers' direction, while avoiding detection

by banks and law enforcement. As detailed in the PSR, Obiora and his co-conspirators

accomplished these objects by, among other things: (i) stealing personally identifiable

information ("PII") from individual victims, including Victim 1; (ii) obtaining fraudulent driver's

licenses bearing the individual victims' PII and Obiora's and others' photographs; (iii) using the fraudulent identification documents to incorporate Massachusetts businesses, such as a logistics business bearing Victim 1's initials (¶ 35); and (iv) opening bank accounts in the names of those businesses that could be used to received BEC proceeds, such as an account in the name of a landscaping business bearing Victim 2's name (¶¶ 28a-28d, 41). Instead of stealing identities to open bank accounts, Obiora sometimes recruited co-conspirators to open purported businesses in their own names, such as CC-3's purported painting business or CC-4's purported design business (¶¶ 42, 48), or to permit Obiora to use their actual businesses and bank accounts to receive BEC proceeds. (¶¶ 28e-28f).

By text message, Obiora provided bank account numbers to co-conspirators in Nigeria and elsewhere. The co-conspirators sent those account numbers on to scam victims as the bank accounts to which the victims should re-direct wire transfers. (¶ 28g). Obiora was aware that "hackers" were involved in stealing the money that would be deposited, and that the hackers (for their role in tricking the victims) and Obiora and his co-conspirators (for their role in laundering the proceeds) would earn similar amounts from the scheme. (*e.g.*, ¶ 28p & n.1(f)) ("So you guys 40%, filer (hacker) 40%, middlemen (…) 20%)). In one text message to a co-conspirator, after proclaiming "I'M RICH", Obiora sent a screenshot claiming a 25 percent share of $800,000 in BEC proceeds. (¶¶ 75-76).

Obiora and others monitored the conspiracy's bank accounts for the arrival of stolen funds, and messaged co-conspirators screenshots of accounts balances showing that the stolen money had arrived. (¶ 54). When those funds arrived, the co-conspirators quickly withdrew the money—by check, wire, and other financial transactions—before BEC scheme victims learned that they had been tricked and succeeded in reversing or freezing the money they had transferred.

(¶¶ 28h-28j). Obiora and others then wired the scheme's proceeds on to other bank accounts and overseas, including to China, Germany, and Nigeria. (¶¶ 28l, 62, 72, 77).

To conceal the existence of the conspiracy, Obiora and others acting at his direction forged business invoices and wrote false memos on checks to suggest that the BEC scheme proceeds they were receiving were legitimate business revenues. For example, shortly after a victim company wired $800,000 to an account Obiora controlled in the name of a landscaping business, Obiora caused the account to issues three checks totaling $773,000, each with a residential address written on the memo line. (¶¶ 74a-74c). Obiora and co-conspirators also lied to banks about the true source of the victims' funds. (¶¶ 28n-28o). For example, on or about March 23, 2021, Obiora instructed CC-2 to call JPMorgan Chase and "ask them why they reversed the two checks [for $109,000] you wrote. Just in case they ask where the 110 came from tell them it came from an investor whose [sic] investing in [your] company to buy new trucks and equipment." (¶ 61).

The victims lost significant amounts of money—often in the hundreds of thousands of dollars. *See*, *e.g.*, Victim 1 (~$110,000, ¶ 59); Victim 2 ($217,000, ¶ 68); Victim 3 ($800,000, ¶ 74); Victim 5 ($375,000, ¶ 80). As noted above, the actual losses to approximately 30 BEC scheme victims were more than $3.3 million. (¶ 85). At a 40 percent commission, Obiora and his U.S.-based conspirators earned a more-than $1.3 million share. (¶ 28p).

B.   *The Offenses - The Passport Fraud Conspiracy*

Less than a year into the money laundering conspiracy, Obiora was removed from the United States to Nigeria as the result of prior drug trafficking conviction. (¶ 129). From Nigeria, as noted above, Obiora continued to lead the money laundering conspiracy. Obiora also agreed with a Boston-area relative to obtain a U.S. passport that would permit Obiora to return to the

United States without permission. (¶ 18). The relative falsely reported their passport lost and applied for a replacement in the relative's name, but the relative used Obiora's picture on the application. (¶¶ 19-20). The relative then sent the passport to Obiora, (¶ 22), who used it to attempt to enter the United States at Detroit's international airport, where he was arrested after arriving on an inbound flight from Cancun, Mexico. (¶¶ 23-26).

C.   *The Recommended Sentence*

The United States has recommended that the Court sentence Obiora to 168 months in prison, with credit for time served since October 11, 2023. As set forth below, each of the factors set forth at 18 U.S.C. § 3553(a) counsels in favor of a significant sentence.

1.   *Seriousness of the Offense*

Obiora was a vital player in a significant money laundering organization. While it might be tempting to conclude that the BEC scheme itself is the serious offense (and its architects the most serious offenders), these schemes do not work without access to the U.S. banking system. In evaluating the importance of Obiora's role, the Court need only notice that Obiora and his laundering crew took at least the same percentage profit out of the fraud as the hackers—40 percent—and that Obiora sometimes negotiated more than the hackers' share. (¶¶ 28-29). The allocation makes sense, since the U.S. participants in the scheme are on business incorporation documents, bank account applications, bank surveillance videos, and U.S.-based communication networks to which the government can obtain investigative access.[3]

The victim statements at the beginning of the government's memorandum underscore the kind of disruption and damage Obiora caused. Many of the fraudulently induced wires came

---

[3] Where he negotiated the overall percentage due to the co-conspirators, Obiora's personal profit—itself 25 percent for some transactions—hardly lessens his culpability.

from businesses that could not afford to lose the kind of money involved in them. There is also a human dimension to these corporate crimes. Anyone who has ever been tricked, or made a mistake at work, can imagine the impact of learning that they had just wired six figures in business revenue to the wrong person.

What is more, Obiora's GSR does not reflect the seriousness of his passport offense at all. (¶ 104). This omission would ordinarily be grounds for the Court to sentence at the upper end of Obiora's GSR for his money laundering offense. USSG § 3D1.4, Background ("If there are several groups and the most serious offense is considerably more serious than all of the others, there will be no increase in the offense level resulting from the additional counts. Ordinarily, the court will have latitude to impose added punishment by sentencing toward the upper end of the range authorized for the most serious offense."). Obiora's attempt to evade the consequences of his removal by getting a fraudulent passport and coming back to the United States without permission is serious, as was the cocaine trafficking offense that led to his removal in the first place. (¶ 129). But a 168-month sentence is already significant, and it already reflects the seriousness of Obiora's two offenses of conviction, even if that sentence varies below the otherwise applicable Guideline.

2.   *Individual Deterrence*

Obiora also presents a substantial risk to re-offend, and it is important that the Court's sentence protects the public from him. Obiora's very first adult offense, at age 18, featured both dishonesty (his provision of a false name to the police) and access device fraud (his possession of a bank debit card in another person's name)—criminal themes that have recurred throughout his adult life. (PSR ¶ 115). In short order, and seemingly without interruption in the years that followed, Obiora was convicted of identity theft (¶ 117); drug possession (¶ 118), larceny based

on the theft and deposit of checks (¶ 119), a firearms offense (¶ 121), two more larceny convictions based on the theft and deposit of checks (¶¶ 122-23), two more convictions for uttering and larceny (¶¶ 124-25); two additional convictions involving the provision of false information to police officers (¶¶ 126-27); a cocaine trafficking conviction resulting in a five-to-seven year term of imprisonment (¶ 129); and an assault conviction for punching a corrections officer while in custody (¶ 130). At least two of his offenses, including Obiora's offense of conviction on Count 2 of the Superseding Information, took place while he was under a criminal justice sentence. (¶ 132).

It can be fairly said that some criminal history scores overstate a defendant's culpability, his past involvement with the criminal justice system, and the likelihood of recidivism. Obiora's is not one of them. A significant sentence of imprisonment is necessary in this case because past terms of imprisonment for financial offenses have not deterred Obiora from re-offending.

Obiora's direction of most of this scheme from abroad, including by recruiting co-conspirators to receive BEC proceeds in bank accounts and directing their activities, indicates that he is an even more serious risk to re-offend. At the conclusion of whatever term the Court imposes, Obiora will be removed to Nigeria again. He is likely to face the same economic and social pressures that led him to defraud others and to attempt to re-enter the United States. At that point, the Court will not be able to protect the public from Obiora. A sentence of 168 months meets the need in this case for individual deterrence.

3.   *General Deterrence*

"Considerations of deterrence argue for punishing more heavily those offenses that either are lucrative or are difficult to detect and punish since both attributes go to increase the expected benefits of a crime." *United States v. Zukerman*, 897 F.3d 423, 429 (2d Cir. 2018). Obiora's

crime is particularly suited to a general deterrent sentence, as it was incredibly lucrative, and but for his return to the United States, nearly impossible to punish.

When, as in this case, law enforcement is able to arrest and convict a culpable overseas defendant, it is vital that the sentence imposed reflect a deterrent component. There are so many fugitives from Nigeria because it is a country from which many cybercrimes, including BEC frauds, are committed. Extradition from Nigeria is a long process that does not always result in defendants arriving into U.S. custody, which leaves the government to rely on the chance that a culpable target will travel, as happened here. In such circumstances, only the likelihood of a lengthy jail sentence will deter the next BEC scheme hacker or money launderer. *See United States v. Volynskiy*, 431 Fed. Appx 8, 11 (2d Cir. 2011) (affirming Guidelines sentence "because of the serious nature of defendant's crimes, his important role and long involvement in the scheme, and the need for general deterrence of international hackers"); *United States v. Hatala*, 552 Fed. Appx. 28, 32 (2d Cir. 2014) (affirming Guideline sentence based in part on general deterrence "because of the particular danger posted to increased internet commerce by the type of crime at issue and the difficulty in identifying and locating criminal perpetrators"); *United States v. Watt*, 707 F. Supp. 2d 149, 156-57 (D. Mass. 2010) (Gertner, J.) ("deterrence and punishment are particularly important for cybercrimes"). Judge Rakoff's observations regarding insider trading apply equally to Obiora's commission of a money laundering offense from overseas: "an easy crime to commit but a difficult crime to catch. Others similarly situated to the defendant must therefore be made to understand that when you get caught, you will go to jail." *United States v. Gupta*, 904 F. Supp. 2d 349, 355 (S.D.N.Y. 2012).

The reality is that many BEC scammers are beyond the reach of U.S. authorities and will likely remain so. More modest sentences have failed to serve as an adequate deterrent. The

9

significant sentence requested here should change the cost-benefit analysis for others involved in BEC schemes, and for the co-conspirators Obiora leaves behind in Nigeria.

    4.   *Similarly Situated Defendants*

A 168-month sentence would also fairly reflect how courts punish money launderers like Obiora, both nationally and in this District, even though sentencing data puts Obiora in rare company as an offender. According to Judiciary Sentencing Information, since 2019, there have only been 6 defendants whose primary Guideline was § 2S1.1 (money laundering) and who had a Final Offense Level of 31 and a Criminal History Category of VI. (¶ 192). The government's recommendation in this case, 168 months, is exactly the median sentence among those six historical defendants. The average sentence for this group was similar, at 149 months (¶ 192).

Data from the U.S. Sentencing Commission puts a sentence of 168 months for an offender like Obiora well within the norm. Between 2015 and 2023, of the 15 custodial sentences imposed in this District for which § 2S1.1 was the primary Guideline and the offender was in Criminal History Category VI—without respect to either sentencing departures or the Total Offense Level, which the Sentencing Commission's Interactive Data Analyzer does not track— a full 60 percent of the sentences were 120 months or more. Similarly, 63 percent of these sentences nationally exceeded 120 months.

Within this District, the Court's sentences of <u>first-time offenders</u> who engaged in conduct similar to Obiora are instructive. In *United States v. Kofi Osei*, 21-cr-10064-IT, the defendant opened bank accounts and recruited others to do the same, all to receive more than $3.5 million in fraud proceeds, as in this case. The defendant's Total Offense Level was 31, also like this case. Osei, however, was a first-time offender, with an advisory GSR of 108 to 135 months. The Court sentenced him to 54 months. Obiora is not similarly situated to Osei, however. Osei

committed his offenses here, not from Nigeria after being removed from the United States; he had no criminal history; and he and his co-conspirators earned only approximately 10 to 20 percent of the amounts they received in their bank accounts—less than what Obiora made on his own and less than half the 40 percent profits that went to Obiora's ring. A first-offense variance has no place in this case. *See United States v. Hassan Abbas*, 20-cr-10016-LTS (defendant with no criminal history sentenced to 87 months' imprisonment for opening bank accounts to launder $2 million proceeds of BEC schemes and romance scams); *see also United States v. Charles Ochi*, 22-cr-10255-RGS (first-time offender who recruited others to launder more than $1 million in financial fraud proceeds, at GSR of 70 to 87 months, sentenced to 60 months in prison); *United States v. Omoruyi et al.*, 21-cr-10217-PBS (two first-time offenders who opened bank accounts in the names of fake companies and fake people to launder $2 million in fraud proceeds sentenced to 78 and 72 months, respectively).

<div align="center">5.   History and Characteristics of the Defendant</div>

The government is comfortable recommending a below-Guidelines sentence in part based on defendant's mental health. The diagnoses described in the PSR (¶¶ 156-160a) are serious and appear to have recurred as recently as last month. (¶ 160a). They support a modest variance, as does the fact that Obiora will be again removed from the United States, away from his parents, his children, and other people who used to provide social support here. But his psychiatric diagnoses appear to be controllable with medication, and his symptoms do not seem to have interfered with his ability to oversee serious offenses of conviction. The government respectfully submits that the requested sentence (or one near it) adequately accounts for Obiora's circumstances.

<div align="center">11</div>

CONCLUSION

For all of these reasons, the United States respectfully requests that the Court sentence Chukwunonso Obiora to 168 months' imprisonment, 3 years supervised release (if he is not removed from the United States at the end of his term), and a $200 special assessment. The Court should also order the defendant to pay restitution to the victims of the offense totaling 3,326,014.48 and enter the forfeiture order that will be the subject of a separate motion to the Court. The government does not seek the imposition of a fine.

<div style="margin-left:auto">

Respectfully submitted,

JOSHUA S. LEVY
United States Attorney

By: /s/*Seth B. Kosto*
Seth B. Kosto
Assistant United States Attorney
One Courthouse Way, Suite 9200
Boston, Massachusetts 02210

</div>

December 11, 2024

CERTIFICATE OF SERVICE

I hereby certify that on December 11, 2024, I provided a copy of the foregoing to the attorneys for the defendant through the Court's Electronic Case Filing system.

<div style="margin-left:auto">

/s/*Seth B. Kosto*
Seth B. Kosto
Assistant United States Attorney

</div>

December 11, 2024